computer emergency response team CERT-EU

Security White Paper 2011-002

CERT-EU Services - Fundamentals

Introduction

The CERT-EU delivers IT security services (warnings and announcements, alerts, incident response coordination) to help EU Institutions, Agencies and Bodies to protect their IT assets from cyber-attacks. All of these services require contribution, input and feedback from the constituency. Especially incident response coordination and alerts requires the Institutions to **play an active role**, for example by informing CERT-EU about incidents occurring in their organisation in a timely fashion. A minimum set of best practices are required to optimise CERT-EU's service provision, and keep the Institutions in control of the data exchanged with CERT-EU.

The present paper lays down guidance for participating actively in the services of CERT-EU, for the benefit of all EU Institutions, Agencies and Bodies. This guidance will be complemented by subsequent whitepapers about specific topics.

Why to report to CERT-EU?

One of the core businesses of CERT-EU is the adequate dissemination of information about ongoing attacks or new (critical) vulnerabilities affecting the EU Institutions. Sources of information for detecting ongoing attacks and eventually triggering alerts include:

- Alerts received from CERT-EU peers (e.g. other CERTs),
- Information from open/specialised sources,
- Incidents reported by EU Institutions, Agencies or Bodies.

When a Constituent reports for example an ongoing attack, an infection with malware or even just a targeted social engineering attempt via email, the Constituent itself but also all others will benefit from the resulting alert by CERT-EU for various reasons:

- The reporting Constituent may be part of a larger campaign of attacks targeting others EU Institutions, Agencies and Bodies,
- The attack pattern may not have been detected by other EU Institutions, Agencies and Bodies,
- New attack signatures may not yet be detected by anti-malware tools,
- CERT-EU maintains a comprehensive list of contact information to both constituents and peers (other CERTs, ISPs, etc), and CERT-EU can efficiently coordinate the handling of dissemination of information on incidents on a larger scale.

Therefore Constituents' active participation is essential in early warning and efficient reaction.

How to report to CERT-EU?

To make incident notification as straight forward as possible, CERT-EU recommends to use the following ***template.*** You can also download the template from CERT-EU Website.

START OF MESSAGE
****
PROTECTIVE MARKING AND DISTRIBUTION:
1. Level of sensitivity (select)……..: [LIMITED / EU RESTRICTED[1]]

2. Release authorizations (select)…….: [Personal - for named recipients only
/ Limited distribution (within CERT-EU only)
/ Community wide (within EU Bodies only)
/ Unlimited]

CONTACT DETAILS
3. Organisation…….....:
4. Email address…..……..:
5. Phone number…..…….:

INCIDENT DETAILS
6. Date and local time of incident discovery:
7. Time zone…….....:
8. Current status (select)……...: [Occurring / Contained / Recovered / Unknown]
9. Number of impacted systems (estimated):
10. Description of incident……..……..:
(Whenever the information is easily and already available, you may include as well software version and patch level, the infected or suspicious file(s), how was the incident detected, methods of intrusion, the IP address or URL of the source of incident, intruder tools involved, intruder tool output, details of vulnerabilities exploited or any other relevant information. Please include information you already have, this should not delay the notification of the incident. Further information can be communicated later while the incident is being handled.)

SYSTEM DETAILS
11. Host name or IP...……...…….....:
12. Host purpose or function…..…..……:
(e.g., DNS/web server, workstation, etc.)

REACTION
13. Response actions taken……...……:
14. Other organization contacted……..…...:

EU CERT INTERVENTION
15. EU CERT Action (select)……...: [Information / Assistance / Alert]

16. Follow-up (select)…...…….....: [Initial notification to CERT / Follow-up of previously notified]
****
END OF MESSAGE

In emergency cases, unformatted messages will be accepted as well. In such cases further details on incidents can be forwarded later on.

[1] Appropriate encryption should be applied in line with the data classification.

How to communicate with CERT-EU?

With regards to exchanges between Constituents and CERT-EU, incidents & alerts should be exchanged only via **functional mailbox**. The functional email address to be used for reporting incidents to CERT-EU is: cert-eu@ec.europa.eu.

This will ensure that important messages reach relevant contacts in Constituents, facilitate authentication of messages and need-to-know management.

This functional mailbox will be able to encrypt and exchange encrypted content with CERT-EU whenever required.

What to report to CERT-EU?

In its initial phasing-up period, typical incidents that may be reported CERT-EU include:

- Potential malicious files (e.g. those received as attachment to malicious emails or via incitation to click on malicious links),
- Denials of Service,
- Compromised systems (including in other institutions),
- Scans / probes / attempts to perform any of the above.

Whenever possible, Constituents are strongly encouraged to perform some pre-assessment and filtering of incidents reported internally. This will allow dropping some unconfirmed incidents or spam.

The CERT-EU will always handle the reported information in line with its common information assurance principles (see next chapter).

How to deal with information assurance?

While exchanging data in the context IT security incidents handling, it is important to keep in mind that unauthorised disclosure or lack of authenticity of data can have damaging impact on involved organisations and individuals. Especially in case of targeted attack, the privacy of involved individuals and knowledge of the existence, origin, nature of the attack should be appropriately protected. Furthermore, the targeted organisation must retain control on information related to the attack.

Ownership of information. Constituents will control:

- The sensitivity of information by using appropriate markings (item 1 of template incident message),
- The dissemination of information by using Traffic Light Protocol (item 2 of template incident message), and
- The level of services requested to CERT-EU by selecting level of intervention required (item 15 of template incident message)

The CERT-EU will respect the security marking and the ownership of information, it will coordinate use with the information owner.

Communication security tools. In the short term, the CERT-EU is using PGP for electronic messages encryption and signature. The public key of CERT-EU is:

ID: 0x46AC4383
Fingerprint: 9011 6BE9 D642 DD93 8348 DAFA 27A4 06CA 46AC 4383
Key expires: 01/06/2012

Additionally, another encryption mechanism (ACID) is also being used with some customers.
In the longer term, investigations will be pursued for a standard tool for IT incident exchanges across EU institutions and bodies.

Communication security practices. Electronic exchanges should whenever necessary be protected by the following controls:

- Sanitization: unless necessary for incident handling by CERT-EU, avoid providing details in clear on identity/personal information of individuals, origin/nature of targeted attacks, assessment details. Encrypt the message (see below) or drop such information.
- Authentication: sign messages.
- Confidentiality: encrypt messages and/or attachments, when sensitive data mentioned above are present, or in case you have any doubts about its sensitivity.